

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 2

In the drawings:

Please replace sheet 3 of 4, including FIGs. 3 and 4, with the enclosed replacement sheet 3 of 4.

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 9

REMARKS

Drawings

FIGs. 3 and 4 have been objected to because they present two different tables that are labeled with the same name. As the Examiner has correctly indicated, FIG. 4 denotes a channel key table, and not a channel state table. Applicant has submitted herewith a replacement sheet encompassing FIGs. 3 and 4, in which FIG. 4 properly denotes a channel key table.

Claim rejections under 35 USC 112, first paragraph (enablement) as to claims 1, 8, and 10-14

Claims 1, 8, and 10-14 have been rejected under 35 USC 112, first paragraph, as failing to comply with the enablement requirement. The Examiner has indicated that these claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention. In particular, the Examiner states that the recitation of the term hardware or hardware mechanism, as performing various functionality, within these claims is not enabled, because "the specification does not disclose any particular circuitry of the hardware (for example) that would allow one of ordinary skill in the art [to] determine how the implementation of such . . . hardware could satisfy the claim limitations." (Office action, pp. 3-4, para. 7)

Applicant respectfully traverses this rejection. Applicant submits that the Examiner is holding Applicant to an enablement standard that is not found in case law or the MPEP. First, it is noted that the terminology hardware or hardware mechanism is found throughout the specification as providing the same functionality as to which this terminology is limited to providing within the claim language. (See, for instance, paras. 30, 32, 33, and 54, among other paragraphs) That is, the hardware of the claimed invention is *functionally described* throughout the specification, in language corresponding to that of the claim language.

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 10

Now, the crux of the Examiner's rejection is that the specification does not show how to *implement* such hardware as to which the claimed invention is limited. However, as long as the specification provides disclosure bears a reasonable correlation to the entire scope of the claim, then the enablement requirement of 35 USCC 112 is satisfied. (MPEP sec. 2164.01(b)) "It is not necessary to explain every detail, since the inventor is speaking to persons of ordinary skill [within the art]." In re Wands, 8 USPQ2d 1400 (Fed. Cir. 1988) That is, "[n]ot every last detail is to be described, else patent specifications would turn into production specifications, which they were never intended to be." In re Gay, 135 USPQ 311 (CCPA 1962) Specifications thus "need only be reasonable with respect to the art involved; they need not inform the layman nor disclose what the skilled already possess. They need not describe the conventional. . . . The intricacies need not be detailed ad absurdum." General Elec. Co. v. Brenner, 159 USPQ 335, 337 (D.C. Cir. 1968) (Emphasis added)

Applicant has described throughout the specification what the hardware of the claimed invention functionally does. One of ordinary skill within the art would easily be able to construct such hardware to perform this functionality. There is no need to "explain every detail" within the specification, to provide a detailed circuitry implementation of such hardware, else the patent specification "would turn into [a] production specification." "The intricacies" of such hardware "need not be detailed ad absurdum."

Indeed, the U.S. Supreme Court eloquently summarized the state of the law as to the enablement requirement more than 100 years ago in Webster Loom Co. v. Higgins, 105 U.S. (15 Otto) 580 (1881):

If a mechanical engineer invents an improvement on any of the appendages of a steam-engine . . . he is not obliged, in order to make himself understood, to describe the engine, nor the particular appendage to which the improvement refers, nor its mode of connection with the principal machine. These are already familiar to others skilled in that kind of machine. He may begin at the point where his invention begins, and describe what he has made that is known, and what it replaces of the old. That which is common and well known is as if it were written out in the patent and delineated in the drawings.

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 11

In the present patent application, Applicant contends that the hardware functionally described in the specification is enabled to those of ordinary skill within the art. One of ordinary skill within the art is able to use such hardware, insofar as indeed the functional description of such hardware inherently teaches how to use the hardware. Furthermore, one of ordinary skill within the art would easily be able to implement the hardware that is functionally described within the specification, since constructing hardware to perform given functionality is routinely achieved by those of ordinary skill within the art every day. As a system designer, for instance, I can tell a hardware engineer the functionality that I wish to implement in hardware, and the hardware engineer can easily construct such hardware. As stated by the Federal Circuit in *In re Wands*, it is not necessary to explain every detail of such things known within the art. As stated by the Supreme Court in *Webster Loom*, it is not necessary to explain details that are already familiar to others skilled in that kind of machine.

The Examiner's asking for example circuitry that could implement the hardware that is functionally described within the specification is tantamount to asking for a blueprint. "However, the law does not require a specification to be a blueprint in order to satisfy the requirement for enablement under 35 USC 112, first paragraph." (*Staehelin v. Secher*, 24 USPQ2d 1513, 1516 (BPAI 1992)) Indeed, disclosing hardware *functionally*, as Applicant does throughout the specification, necessarily meets the enablement requirement. "Disclosing a microprocessor capable of performing certain functions is sufficient to satisfy the requirement of section 112, first paragraph, when one skilled in the relevant art would understand what is intended and know how to carry it out." (*In re Hayes Microcomputer Prods. Inc. Patent Litig.*, 982 F.2d 1527, 25 USPQ2d 1241, 1246 (Fed. Cir. 1992)) "Disclosure of apparatus with diagrams describing the function but not the structure of the apparatus is not, per se, fatal under the enablement requirement of 35 USC 112, paragraph 1, as long as the structure is conventional and can be determined without an undue amount of experimentation." (*In re Ghiron*, 537 F.2d 1123, 190 USPQ 402, 405 (CCPA 1976))

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 12

Therefore, the crux of Applicant's response to the Examiner's enablement rejection is that the claimed hardware is functionally described within the specification, and that such functional description is sufficient to enable one of ordinary skill within the art to make and use the claimed invention. Detailed circuitry showing how such hardware can be constructed is not necessary, else the patent specification would improperly turn into a production document. The law does not require the specification to be a blueprint in order to satisfy the enablement requirement. Functional language is sufficient for enabling a specification disclosing and claiming the invention. Indeed, the specification does not need to even contain a working example if the invention is otherwise disclosed so that one of ordinary skill within the art would be able to practice the invention without undue experimentation! (In re Borkowski, 422 F.2d 904, 164 USPQ 642, 645 (CCPA 1970) For all of these reasons, then, Applicant submits that the claimed invention has been sufficiently enabled.

Claim rejections under 35 USC 112, first paragraph (written description) as to claims 1 and 3-8

Claims 1 and 3-8 have been rejected under 35 USC 112, first paragraph, as failing to comply with the written description requirement. In particular, the Examiner has stated that there is no support for only a kernel agent being able to access the hardware. Without prejudice, Applicant has amended the claimed invention to remove this language, and therefore submits that claims 1 and 3-8 satisfy the written description requirement.

Claim rejections under 35 USC 112, second paragraph as to claims 1, 3-8, and 10-18

Claims 1, 3-8, and 10-18 have been rejected under 35 USC 112, second paragraph, as being indefinite. In particular, the Examiner has stated that the limitation that the keys are inaccessible by all user processes suggests that the keys are accessible only for processes other than user processes. Applicant in response states that the Examiner is correct in making this suggestion.

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 13

However, the Examiner goes on to say that the claim language recites that the keys are for establishing a secure transmission channel from a user process of a first node to a user process of a second node, which suggests that the user processes are able to access the keys, such as possibly delegating the accessing functions to other processes. Rather, the Examiner states that Applicant possibly means that the keys are not *directly* accessible to the user processes.

Applicant respectfully traverses this rejection. Applicant means exactly what is written in the claim language of the claimed invention. The user processes have no access to the keys. The Examiner seems to think that because the user processes have no access to the keys, that therefore there is no way a secure transmission channel between two user processes with such keys can be established. However, this is incorrect. The hardware can access the keys to establish a secure channel between two user processes, but this does not mean that the user processes have even indirect access to the keys – the user processes still cannot access the keys even when the hardware accesses them to establish the secure channel between the user processes.

Applicant notes that “in rejecting a claim under the second paragraph of 35 USC 112, it is incumbent on the examiner to establish that one of ordinary skill in the pertinent art, *when reading the claims in light of the supporting specification*, would not have been able to ascertain with a reasonable degree of precision and particularity the particular area set out and circumscribed by the claims.” (Ex parte Wu, 10 USPQ 2031, 2033 (BPAI 1989)) That is, it is well settled that the language of the claims, *read in light of the specification*, is to be considered when determining whether the claims are definite. (Allen Archery Inc. v. Browning Mfg. Co., 819 F.2d 1087, 2 USPQ2d 1490, 1494 (Fed. Cir. 1987)) “It is important here to understand that under this analysis claims which on first reading – in a vacuum, if you will – appear indefinite may upon a reading of the specification disclosure or prior art teachings become quite definite.” (In re Moore, 439 F.2d 1232, 169 USPQ 236, 238 n.2 (CCPA 1971))

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 14

Applicant thus submits that, in reviewing the claim language in light of the specification, as is required in the indefiniteness inquiry, it is clear that the claim language at issue here is indeed quite definite. Throughout the specification, the process by which a secure transmission channel is established between two user processes where the user processes do not have access to the keys is definitively described. (See, for instance, para. 29, which describes that such a secure channel is provided, and para. 25, which notes that the key is inaccessible to the user processes.) That is, the specification shows how the hardware accesses the keys to establish a secure channel between two user processes, and that even with such hardware access, the user processes never have access to the keys, period. Therefore, the claim language that has to be interpreted in light of this disclosure is indeed definite under 35 USC 112, second paragraph.

Applicant provides a corresponding example that informs this definiteness discussion. Say that Joe User wants to make a phone call to Frank User. However, it is preordained that Joe User does not have access to Frank User's phone number. Furthermore, it is preordained that Frank User has a phone that is identified by the phone number – but that Frank User does not know, and indeed does not have access to, this phone number. Thus, Frank User could not tell Joe User in advance his phone number for Joe User to call. Therefore, how can Joe User make such a phone call to Frank User? Well, say that Bob Hardware, and only Bob Hardware, has access to Frank User's phone number. Joe User asks Bob Hardware to call Frank User's phone number, so that Joe User can talk to Frank User. Bob Hardware does this, and after calling Frank User's phone number on a phone, gives the phone handset to Joe User so that Joe User can talk to Frank User. Now, neither Joe User nor Frank User has access to Frank User's phone number – only Bob Hardware does. And yet, a phone call is established between Joe User and Frank User, by Bob Hardware. This example shows how hardware – “Bob Hardware” – is able to have access to a key – the phone number of Frank User – to establish a secure communication channel – a phone call – between two users, even though these users – Joe User and Frank User – do not have access to the key. At no point do Frank User and Joe User ever learn what the key “is” – that is,

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 15

at no point do Frank User and Joe User obtain the identity of the key, and thus at no point do Frank User and Joe User *access* the key. Key access is thus not necessary to establish a secure communication between user processes, such that definiteness is satisfied.

For all of the above reasons, then, Applicant submits that the claimed invention as currently delineated in the claims is definite. That said, Applicant wishes to advance the present patent application to issuance as soon as possible. If the Examiner believes that amending the claim language such that the user processes do not have “direct” access to the key would render the claimed invention patentable insofar as 35 USC 112 is concerned – including that such amendment to the claims is supported in the specification inherently or implicitly – then Applicant is amenable to such amendment. In this respect, the Examiner is encourage to contact Applicant’s representative, Mike Dryja, at the phone number listed below.

Claim rejections under 35 USC 103(a)

Claims 1, 3-4, 7, 10-12, and 15-16 have been rejected under 35 USC 103(a) as to Stein (“Web Security . . .”, 1998, ISBN 0201634899) in view of Pfleeger (“Security in computing,” 1996, ISBN 0133374866), and further in view of Carter (5,845,331) or alternatively in view of Fontana (“Defending against Outlook viruses”). Claim 8 has been rejected under 35 USC 103(a) as to Stein in view of Pfleeger and Carter and further in view of Boden (6,182,228) or alternative in view of Fontana. Claims 13-14 and 17-18 have been rejected under 35 USC 103(a) as being unpatentable over Stein in view of Pfleeger and further in view of Benedyk (2001/0055380) or alternatively in view of Pfleeger and Fontana and further in view of Benedyk (2001/0055380) and Bean (4,843,541).

Applicant notes that claims 1, 11, and 15 are independent claims, from which the remaining pending claims depend. Applicant asserts that claims 1, 11, and 15 are patentable, such that the remaining pending claims are patentable for at least the same reasons. Applicant

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 16

specifically discusses claim 1 as representative of independent claims 1, 11, and 15 insofar as patentability over Stein in view of Pfleeger and further in view of Carter or Fontana is concerned.

Claim 1 is limited to a key sent by hardware of a first node to hardware of a second node, where all user processes have no access to the keys. Applicant again refers the Examiner to the reference "Kernel Extensions and Device Support Programming Concepts," filed with the previous office action response, for information as to the distinction between user processes and kernel processes, as discussed in detail in the previous office action response.

Now, the Examiner has stated that Stein teaches a key sent by hardware of a first node to hardware of a second node. Applicant does not necessarily agree, but rather focuses on a second aspect of the rejection. That is, the Examiner has stated that Stein does not explicitly teach that the keys are inaccessible by all user processes. Rather, the Examiner has relied upon Pfleeger as teaching that user processes not having access to keys, such that Stein in combination with Pfleeger teaches a key sent by hardware of a first node to hardware of a second node, where the key is inaccessible by user processes. (Carter and Fontana are also relied upon by the Examiner, to teach that unauthorized processes do not have access to the key, and although Applicant does not necessarily agree, Applicant does not focus on this third aspect of the rejection.)

Applicant, however, submits that Stein is not combinable with Pfleeger, such that the claimed invention cannot be rendered obvious over Stein in view of Pfleeger and further in view of Carter and/or Fontana. In particular, combining Pfleeger with Stein changes the principle of operation of Stein. This is now discussed in detail.

Stein notes that "[t]he *browser* encrypts the [premaster] secret using the server's RS public key" in paragraph 6 on page 42. A browser is a user process, as can be appreciated by those of ordinary skill within the art (i.e., it is definitely not a kernel process, as is also readily understood by those of ordinary skill within the art) and thus has access to the secret that the Examiner identifies as the key sent from the first node to the second node, inherently while it is encrypting the secret. Although it should be readily evident that a browser is a user process and

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 17

not a kernel process, see also page four of the "Application Architecture" reference that has been provided with the previous office action response, in which it is said that a "client can be a Web browser or other end-user process." (P. 4)

Therefore, the principle by which Stein operates is that a particular type of user process, a web browser, has access to the key in order to encrypt communications. Now, the Examiner has cited Pfleeger as teaching that a user process does not have access to a key "to increase system[] security." (Office action, p. 7. para. 21) Therefore, if you modify Stein per Pfleeger, Stein no longer operates according to its principle, in which the web browser has access to the key in order to encrypt communications. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious." (MPEP 2143.01.VI.)

More particularly, the *In re Ratti* decision states that where the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference]," then there is no *prima facie* obviousness. (270 F.2d 810, 813, 123 USPQ 349, 352 (CCPA 1959)) Here, it is instructive to compare the basic design of Stein as evidenced in FIG. 3.2 thereof with the reconstruction that would be required as per Pfleeger as evidenced in FIG. 7-20 thereof. That is, as Stein currently operates, encryption entirely occurs within the user processes block of FIG. 7-20 of Pfleeger. This is because a web browser is a user process. By comparison, if you require that encryption occur in Stein within the security functions block of FIG. 7-20 of Pfleeger, you would have to completely redesign the web browser – and indeed, the operating system on which the web browser runs, the operating system kernel, and the security kernel.

That is, the web browser of Stein would not have access to the encryption key, so it would have to be redesigned and reconstructed to submit requests for encrypted communication to the operating system in FIG. 7-20 of Pfleeger, which would have to be redesigned and reconstructed to receive such requests. The operating system of Stein on which the web browser

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

Page 18

runs would further have to be redesigned and reconstructed to convey such requests to the operating system kernel in FIG. 7-20 of Pfleeger, which would have to be redesigned and reconstructed to receive such requests. The operating system kernel would further have to be redesigned and reconstructed to convey such requests to the security kernel in FIG. 7-20 of Pfleeger. Finally, the security kernel would have to be redesigned and constructed to receive and act upon such requests. That is, the security kernel would have to be redesigned and reconstructed completely to take over encrypted communication functionality for the web browser of Stein.

That is a lot of redesign and reconstruction that needs to be done! It is definitely fair to say that such redesign and reconstruction of the web browser of Stein, of its underlying operating system, and of the operating system kernel and the security kernel would be "substantial." That is, no existing prior art web browser, such as Internet Explorer, could be easily modified to achieve the combination that the Examiner proffers. Rather, such a redesign and reconstruction would be substantial, changing the principle of operation of the web browser and underlying operating system of Stein, per Pfleeger, so that encryption and key access is achieved, not in the web browser as is the principle of operation in Stein, but rather is in the operating system security kernel as in Pfleeger. That is, if you modify Stein in view of Pfleeger, Stein's web browser can no longer encrypt communications itself, which is Stein's purpose in having a web browser have access to the key, and such modification would impermissibly require a substantial redesign and reconstruction of Stein as well.

In other words, while it is easy to say that you could redesign and reconstruct the web browser of Stein so that user processes, like Stein's web browser, do not have access to encryption keys, in practice a substantial amount of redesign and reconstruction would be required to make that happen – to the point where Stein would no longer operate on the principle that is intrinsic in Stein, where the web browser has access to the key and performs encryption itself. Because the MPEP and case law say where such redesign and reconstruction of the

Joseph
Serial no. 09/876,351
Filed 6/6/2001
Attorney docket no. BEA920010008US1

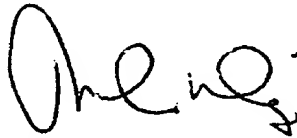
Page 19

primary reference (in this case, Stein) would be substantial, and where such redesign and reconstruction would change the principle of operation of the primary reference, that the primary reference cannot be combined with or modified per the secondary reference (in this case, Pfleeger), Stein is not combinable with Pfleeger. As such, the claimed invention is not rendered obvious over Stein in view of Pfleeger and further in view of one or more other references.

Conclusion

Applicants have made a diligent effort to place the pending claims in condition for allowance, and request that they so be allowed. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney so that such issues may be resolved as expeditiously as possible. For these reasons, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,



Michael A. Dryja, Reg. No. 39,662
Attorney/Agent for Applicant(s)

April 4, 2006
Date

Law Offices of Michael Dryja
704 228th Ave NE #694
Sammamish, WA 98074
tel: 425-427-5094, fax 206-374-2819